CCAOI™

Representing the ecosystem of Internet -Bharat Model

Ref: CCAOI/ TRAI/ CNAP170123/1
17 January 2023

Shri Akhilesh Kumar Trivedi,
Advisor (Networks, Spectrum and Licensing),
Telecom Regulatory Authority of India

Sub: CCAOI's response to TRAI's consultation paper on Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks

Dear Sir,

We thank the TRAI for providing us the opportunity to provide our comments on the consultation paper on the Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks.

CCAOI is a trust, engaged in capacity building, research and advocacy mostly in India especially related to Internet and digital policies. We represent the interest of different stakeholders of the Internet ecosystem in India, including connected and unconnected users. For over a decade CCAOI, has been advocating, organising capacity building initiatives, webinars, conferences, events and conducting research on issues related to internet governance, telecom and digital policies.

We submit that while the CNAP proposal is well intended to address the issue of unsolicited and fraudulent calls, it may not serve to achieve these objectives, and potentially raise new concerns.

We believe that the discussion on CNAP is too premature. TRAI should first conduct a pilot to ascertain the feasibility of CNAP implementation and do an in-depth cost benefit analysis. However, if TRAI still wants to go ahead to implement the CNAP it should be done only after the implementation of the Data Protection Law in India, be an alternative and voluntary 'opt-in' service.

Please find enclosed our submission.

Thanking you and looking forward to favourable consideration of our suggestions in the interest of growth of the digital ecosystem in the country.

With Regards,

Amrita Choudhury
Director CCAOI
amritachoudhury@ccaoi.in

CCAOI™

Representing the ecosystem of Internet -Bharat Model

CCAOI's response to TRAI

on

Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks

We from CCAOI believe the issue of unsolicited and fraudulent calls resulting in financial frauds needs to be addressed.

We therefore thank the Telecom Regulatory Authority of India (TRAI) for trying to address the genuine issue of spam and fraudulent calls and provide safe telephone communications to consumers.

In that context TRAI) released a consultation paper the "Introduction of Calling Name Presentation (CNAP) in Telecommunication Networks" where it proposed a need to display the name of the calling party on the called party's telephone to address this issue.

While the initiative aims to provide users a much-required relief from spam and fraudulent calls by implementing a KYC based caller identification system, we believe the implementation of this initiative raises several concerns and implementation of the same may not be as straightforward as envisaged.

Implementation Challenges

The CNAP function, to be implemented by the Department of Telecommunications (DoT), plans to establish a model that can be employed across various technology networks and service providers, without the requirement for the internet or smartphones. However, the readiness of the telecom network and the practicality of providing CNAP to all telephone subscribers is a complex undertaking. TRAI has proposed four different models for the implementation of CNAP in a technology-neutral and internet-independent manner, but the issue is still intricate.

1. The current networks, both wireless and landline, vary greatly. While modern networks may support CNAP supplementary services, older networks may pose issues and there may be discrepancies between different network types.
2. Telephone handsets in India may require software upgrades to enable CNAP. Collaboration between multiple stakeholders, such as manufacturers and service providers, will be necessary to enable CNAP on future supplies and the impact on current products is uncertain.
3. The DoT will need to amend existing provisions or include new provisions in telecom service licenses/authorizations concerning CNAP as there is currently no mandate in existing licenses.

Financial Implications

Secondly, the enhancement of systems and networks would incur a financial cost for telecommunications companies which may not be proportional to the anticipated outcomes.

Issues related to balancing Transparency with consumer privacy and choice

Thirdly, there is a need to balance transparency with protecting the privacy and autonomy of telecom subscribers. TRAI's proposal to make the display of Calling Name Presentation (CNAP) mandatory for telcos has the potential to restrict consumer choice and invade individual privacy.

It is important to note that Telcos are already mandated to display Caller Line Identification (CLI). TRAI's proposal to expand this by mandating the disclosure of personal names of telecom subscribers based on their KYC documentation, poses a significant privacy risk for individuals who may prefer not to be identified to the caller for various reasons (e.g. risk to life and property, witness protection, whistle-blower protection, risk of retribution etc.).

The mandatory nature of the CNAP feature poses a risk of unauthorized disclosure of personal information and potential misuse of personal information. For example, this system poses risks to female subscribers. There is a risk of unauthorized disclosure of personal data, as her name will be displayed to the receiver, regardless of her consent to such display. This could potentially mean that bad elements in society can have access to her name and number and expose her to harms such as her number being circulated among other nefarious elements, targeted sexual harassment, spam through calls and messages, and so on.

Limitations of KYC based Solution

The issue of unsolicited calls is a complex matter and cannot be resolved solely by relying on the KYC information provided when issuing a SIM. To tackle the problem of unsolicited calls, TRAI and DOT have implemented multiple measures such as Do Not Disturb, TCCCPR 2018, etc, but the problem persists.

Although telcos comply with mandatory KYC compliance checks of users prior to the issuance of SIM cards by filling out the Customer Acquisition Form (CAF) and collecting supporting KYC documents and verifying basic user information (full name, photograph, DoB, address, etc.) based on certain officially valid documents (e.g., Aadhar, driving license, PAN, passport, etc.), there are many examples of fake identity cards being used for issuing SIM cards.[1]

Reasons for this anomaly include errors in manual verification of KYC, lack of universal digital verification of KYC, SIM not being purchased by the actual user, etc. The current rules also allow any individual to obtain up to 9 SIM cards by providing their proof of identity and proof of address. For example, an individual could purchase a SIM using their ID and then give the SIM to their parent, siblings, children or someone else who would not be in the KYC database. In case the individual purchasing the SIM has fake IDs, the KYC will also not be able to verify it. The KYC, therefore, overlooks that an individual purchasing the SIM may not necessarily be the user of the number.

Such incorrect identification is likely to lead to more confusion and TRAI should consider the consequences of incorrect identification due to the proposed KYC solution.

[1] https://www.bgr.in/telecom/vi-blocks-nearly-8000-sim-cards-issued-on-fake-identity-proof-1250015/

CCAOIs suggestions:

Given India's distinct user base, technical complexities, etc. it is suggested that before discussing the implementation of CNAP, more research on its pros and cons be conducted. Before even contemplating the mandate of CNAP, it is suggested that TRAI:

Pilot Program

Conducts a pilot program in a restricted region to gain practical knowledge and first-hand experience of the benefits/ difficulties in executing the CNAP. This type of research based on real-life evidence will assist TRAI to not only comprehend the actual situations but also put forward an India-specific feasible solution.

Cost Benefit Analysis

Conduct a cost-benefit analysis related to the implementation and upkeep of the CNAP infrastructure and database. Such an analysis will aid in determining whether the implementation of CNAP or an alternate solution will aid in addressing the problem of spam and fraudulent calls the regulator wishes to resolve and estimate the additional financial burden the telcos and/or the government will have to endure.

Explore Alternative Solutions

Instead of solely relying on a KYC-based identification solution which has its limitations as previously mentioned, TRAI should investigate existing or alternative solutions or technologies to provide precision for caller ID systems. For instance, the regulator should examine the existing solutions that are available in the market such as crowd-sourced data solutions, and deliberate along with telcos and such solution providers on how these solutions can be improved and utilized in conjunction with the current prevalent practices.

Conclusion

We believe that the discussion on CNAP is too premature. TRAI should first conduct a pilot to ascertain the feasibility of CNAP implementation and do an in-depth cost benefit analysis.

However, despite the above considerations, if TRAI still wants to go ahead to implement the CNAP without doing a pilot or a cost benefit analysis, we prefer the Option 1, along with the following suggestions.:

- CNAP should be implemented only after the Data Protection Law in India comes into effect so that the rights of users can be protected and there can be an assessment of its impact on individual privacy.

- CNAP should be introduced as an alternative and voluntary ‘opt-in’ service and not made mandatory for users as proposed. User should be allowed to voluntarily ‘opt-in’ for such a CNAP functionality (with an option to withdraw their consent at any time in an easy manner). Such a voluntary and express ‘opt-in’ would not only preserve consumer-choice but would also ensure that the constitutionally protected fundamental

rights are respected and given necessary and due policy protection both in letter and in spirit.

- For security of the data and avoid any single point failure, the CNAP database should not be centralised but distributive in nature. Perhaps each telco should manage their own set of data.